Amendments to the Specification:

Please replace the paragraph beginning at page 19, line 11, and ending at line 29, with the following amended paragraph:

--When the primary message arrives at route point processor 308, acknowledgement is sent by the primary route point processor ~~309~~ 308 to source connector 302 indicating receipt of the primary message ~~has been received~~. Similarly, receipt of the secondary message is acknowledged by the secondary route point processor 310. Once receipt is acknowledged, each route point processor sends a confirmation to the source connector and then replicates the message and sends one to the archive. The primary route point processor sends the replicated message to the primary archival database 314 and the secondary route point processor sends its replicated message to secondary archival database 316. Each route point processor[[s]] also attempts to independently transmit the message to the destination connector 306, again along separate and distinct communication backbones. While it is clearly feasible to utilize merely a single communication backbone and route point processor to complete the transmission of a message from the source to the destination connector, such a configuration would be inherently unreliable as will be explained in greater detail below. To both guarantee delivery and minimize the time to complete the delivery, the present system and method invokes separate and distinct transmission paths, duplication of messages and duplication of system components while sacrificing the expense associated with the increased usage of available bandwidth.--

Please replace the paragraph beginning at page 28, line 4, and ending at line 14, with the following amended paragraph:

-- Referring now to Figure 2A[[B]] that illustrates a connector that is not positioned behind a firewall so that the connector appears on the network as a http proxy interface. Specifically, routing processor 202 is accessible to users via any Internet web browser 204. In this embodiment, the routing processor 202 acquires the log-in name and authenticates the password before passing messages on to the primary and secondary route point processor. Using the log-in information, the routing processor ~~portion~~ 202 first transfers the log-in data to the primary and secondary route point processor using a secure socket layer (SSL) connection. Upon receiving authorization from network controller 108, the connector is configured for the specific user associated with the browser. When security is necessary, the log-in information may be wrapped at the browser 204 in an

encrypted envelope.--